修 士 論 文 の 和 文 要 旨

研究科・専攻	電気通信大学大学院　電気通信学研究科　情報工学専攻　博士前期課程		
氏　　名	山崎　大輔	学籍番号	０７３１０４７
論 文 題 目	コールスタック検査による Windows 版異常検知システム		

要　　旨

近年、不正なプログラムによる攻撃はますます巧妙化しており、攻撃に対する防衛策が盛んに発表されている。中でも、攻撃を検知して管理者等に警告を発するシステムである侵入検知システムが注目を集めている。侵入検知のための手法には様々なものがあるが、現在最も広く用いられているのは、攻撃を特徴づけるパターンとのパターンマッチによる侵入検知である。しかし、この手法には、自己改変型や新種のウイルス、未知の攻撃手法に対して効果が薄いという欠点がある。一方、正常時のアプリケーションのふるまいを覚えておいて、それにマッチしないものを異常と判断して検知するシステムの研究がある。このような研究は、これまで UNIX を対象として多く報告されてきたが、Windows を対象とした発表は少ない。

本研究では、UNIX で高い効果を上げた異常検知手法を Windows を対象として実装し、その有効性を評価することが目的である。手法としては、Feng らによる仮想パス法を用いる。この手法は、システムコール時のコールスタックの内容から、プログラムの抽象的な実行履歴を取得して、プログラムの実行が正常か異常かの判断を行うものである。

本手法を Windows に適用するにあたっては、いくつかの問題がある。一つは、Windows には、UNIX における ptrace のように、簡単にシステムコールをフックするための機構が備わっていないことである。この問題を解決するため、本研究では、Windows 上でシステムコールをフックするための複数の機構を比較検討し、その中から、良好であると考えられるものを実装した。もう一つの問題は、Windows では、コールスタックから実行履歴に関する完全な情報を取得できない場合があることである。調査の結果、この問題を根本的に解決するのは単純ではないことがわかったため、上記の場合には、部分的な情報のみに基づいて正常か異常かの判断を行うこととした。

本研究の異常検知システムによる監視を行いながら、現実的なアプリケーションを実行し、検知精度を測る実験を行った。その結果、高精度で異常検知ができることを確認した。